## REMARKS

Claims 1-18 are pending in this application. Claims 1-18 have been amended. No new matter has been added.

### Declaration

The Declaration submitted was allegedly defective. Applicants submit concurrently herewith a copy of the executed Declaration in the English language.

### Information Disclosure Statement (IDS)

The IDS was partially defective because copies of portions of two non-patent literature documents were not included. An IDS with copies of the missing documents is submitted concurrently herewith for the Examiner to consider.

### Specification Objections

The specification and Abstract were objected to because of informalities. Appropriate corrections have been made. No new matter has been added. Accordingly, Applicants respectfully request that the objections to the specification be withdrawn.

### Claim Objections

Claims 2-18 were object to because of various informalities. Appropriate corrections have been made to place the claims in a more conventional U.S. format. No new matter has been added. Accordingly, Applicants respectfully request that the claim objections be withdrawn.

**Drawing Objections**

The drawing was objected to because of several informalities. The brief description of the drawing may be found on page 11, lines 25-26. There is a single figure that shows a high-level diagram of a system for carrying out the claimed methods.

The reference letters "C" and "M" in the drawing have been replaced with their non-abbreviated equivalents from the specification that identify these letters, namely, "Calculations" and "Mobile telephone." No new matter has been added.

The claimed "communication means" refers to the connections between the processes contained in the box outlined with a dotted line in the figure.

Accordingly, the objections to the drawings should be withdrawn.

**Rejections Under 35 U.S.C. §§ 101 and 112**

Claims 13 and 14 were rejected under 35 U.S.C. § 101 and 35 U.S.C. § 112, first paragraph. Applicants respectfully submit that the amendments to claims 13 and 14 overcome this rejection. No new matter has been added.

**Rejections Under 35 U.S.C. § 103**

Claims 1-6 and 8-18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Futa U.S. Patent No. 7,130,422 in view of Hopkins U.S. Patent Pub. No. 2005/0190912 A1. Claim 7 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Futa in view of Hopkins, and in further view of Matyas U.S. Patent No. 4,736,423. Applicants respectfully traverse these rejections.

Applicants' claims are directed to a method of generating electronic keys for a public-key cryptography method using an electronic device. The claims also relate to a secure portable object using the method. In a first of two separate calculating steps, pairs of prime numbers (p, q) are calculated and stored independent of knowledge of the pair of values (e, l), in which e is the public exponent and l is the length of the key of the cryptography method. The second step is very quick and can be executed in real time by the device, in which a key, d, is calculated from the results of the first step and knowledge of the pair (e, l).

The claims relate more particularly to the generation of keys for an RSA-type cryptography system and to their storage on a secure object with a view to using them in an application requiring security. The claims apply most particularly to secure objects that do not have a large memory resource, such as an electrically programmable memory, or powerful calculation resources, as is the case for chip cards. One embodiment includes electronic commerce using a mobile telephone. In this context, the keys may be on the SIM card of the telephone.

The claimed embodiments address a problem of calculation complexity associated with managing the generation of keys and also the problem of the lack of flexibility due to the initial and definitive storage of a large number of keys and certificates during a personalization phase.

To this end, one embodiment relates to a method of generating electronic keys, d, for a public-key cryptography method using an electronic device, mainly characterized in that it comprises two separate calculation steps:

Step A, which includes 1) calculating pairs of prime numbers (p, q) or values representative of pairs of prime numbers, this calculation being independent of

knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, l also being the length of the modulus N of said method, and 2) storing the pairs or values thus obtained; and Step B, which includes calculating the key, d, from the results of step A and knowledge of the pair (e, l).

Accordingly, the claimed embodiments provide a method involving two separate steps, in which the second step, which can be very quick compared to known solutions, can be carried out in real time. This claimed embodiments also takes up a relatively small amount of memory space. Moreover, there is no limit in terms of new applications not provided at the time of personalization of the card.

Applicants respectfully submit that the same combination of elements is neither disclosed nor suggested by Futa, Hopkins or Matyas, viewed alone or in combination. For example, various sections of Futa (col. 8, lines 56-57, 62-64; col. 9, lines 44, 54-56; col. 10, lines 8, 10, 41-43 and col. 1, lines 65-67) are cited for support of the claimed process where pairs of prime numbers (p, q), or values representative of pairs of prime numbers, are calculated and stored independent of knowledge of the pair of values (e, l), in which e is the public exponent and l is the length of the key of the cryptography method. Applicants respectfully disagree. Indeed, the Action points to nothing in Futa where pairs of prime numbers (p, q) are calculated and stored independent of knowledge of the pair of values (e, l). Futa is simply directed to generating two primes and using a multiplication of the two primes.

Hopkins, which is cited only for allegedly providing a communications means, does not cure the deficiencies of Futa. Moreover, Hopkins, in the cited sections, merely discloses that a recipient may publish his or her public key. Thus, Applicants respectfully submit that the cited sections of Hopkins do not adequately teach or

suggest the claimed communication means for receiving at least one pair of values (e, l).

Accordingly, independent claims 1 and 12 are allowable over the cited references. This logic also disposes of the rejections of claims 2-11 and 13-18, which depend directly or indirectly from claims 1 and 12. Claim 7 is also separately allowable because Futa and Hopkins are cited for teachings they do not provide and Matyas does not compensate for these deficiencies.

**Conclusion**

For the foregoing reasons, Applicants respectfully submit that this application is in immediate condition for allowance and all pending claims are patentably distinct from the cited references. Reconsideration and allowance of all pending claims are respectfully requested.

In the event that there are any questions about this application, the Examiner is requested to telephone Applicants' undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 15, 2008 By: /Brian N. Fletcher/
Brian N. Fletcher
Registration No. 51683

Customer No. 21839